Dynamic Newton-Puiseux Theorem
Bassel Mannaa
Thierry Coquand

Abstract: A constructive version of Newton-Puiseux theorem for computing the Puiseux expansion of algebraic curves is presented. The proof is based on a classical proof by Abhyankar. Algebraic numbers are evaluated dynamically; hence the base field need not be algebraically closed and a factorization algorithm of polynomials over the base field is not needed. The extensions obtained are a type of regular algebras over the base field and the expansions are given as formal power series over these algebras.

2000 Mathematics Subject Classification 03F65, 14Q05,68W30 (primary); 12Y05, 12E05, 12F05 (secondary)

Keywords: Newton-Puiseux theorem, Algebraic curve, Constructive algebra

Introduction

Newton-Puiseux Theorem states that, for an algebraically closed field $K$ of zero characteristic, given a polynomial $F \in K[[X]][Y]$ there exist a positive integer $m$ and a factorization $F = \prod_{i=1}^{n}(Y - \eta_i)$ where each $\eta_i \in K[[X^{1/m}]]$[$Y$]. These roots $\eta_i$ are called the Puiseux expansions of $F$. The theorem was first proved by Newton [8] with the use of Newton polygon. Later, Puiseux [9] gave an analytic proof. It is usually stated as: The field of fractional power series $^1$ , i.e. the field $\bigcup_{m\in\mathbb{N}} K((X^{1/m}))$ is algebraically closed [10]. Abhyankar [1] presents another proof of this result, the “Shreedharacharya’s Proof of Newton’s Theorem”. This proof is not constructive as it stands, and we explain in this paper how to modify his argument by adding a separability assumption to provide a constructive proof of the result: The field of fractional power series is separably algebraically closed. In particular, the termination of Newton-Puiseux algorithm is justified constructively in this case. This termination is justified by a non constructive reasoning in most references [10, 4, 1], with the exception of [5] (For an introduction to constructive algebra, see [7, 6]).

$^1$Also known as the field of Puiseux series.
Another contribution of this paper is to analyze in a constructive framework what happens if the field \( K \) is not supposed to be algebraically closed. The difference with [5], which provides also such an analysis, is that we don’t assume the irreducibility of polynomials to be decidable. This is achieved through the method of dynamic evaluation [3], which replaces factorization by gcd computations. The reference [2] provides a proof theoretic analysis of this method.

With dynamic evaluation we obtain algebras, triangular separable algebras, as separable extensions of the base field and the Puiseux expansions are given over these algebras. Theorem 3.11 shows that the extensions produced by the algorithm are minimal in the sense that if \( R \) is one such extension and \( A \) is any other algebra over the base field such that \( F(X,Y) \) factors linearly over \( A[[X^{1/r}]] \) for some positive integer \( r \), then \( A \) splits \( R \) which in case \( A \) and \( R \) were fields would be equivalent to saying that \( A \) contains the normal closure of \( R \). But this then shows that \( R \) splits itself, which in case \( R \) is a field is equivalent to saying that \( R \) is a normal extension (Corollary 3.12). Theorem 3.14 will then show that that any two triangular separable algebras \( A \) and \( B \) that splits each other are in fact powers of a some triangular separable algebra, i.e. \( A \cong R^m \) and \( B \cong R^n \) for some triangular separable algebra \( R \) and positive integers \( m, n \).

This algorithm gives less information than Duval’s rational Puiseux expansion algorithm [4] since we can easily obtain the classical Puiseux expansions of a polynomial from the rational ones (Rational Puiseux expansions describe the roots of the polynomial by pairs of power series, i.e. a parametrization, with rational coefficients). In [4] the rational expansions of a polynomial \( F(X,Y) \in K[X,Y] \) is given as long as \( F(X,Y) \) is absolutely irreducible, i.e. irreducible in \( \bar{K}[X,Y] \), where \( \bar{K} \) is the algebraic closure of \( K \). For example the polynomial \( Y^2 - 2 \in \mathbb{Q}[X,Y] \) has no rational expansions. It would be interesting to also justify Duval’s algorithm in a constructive framework. However, to dispense with the assumption of absolute irreducibility one might need to alter the definition of rational expansions.

1 A constructive version of Abhyankar’s Proof

We recall that a (discrete) field is defined to be a non trivial ring in which any element is 0 or invertible. The formal power series ring \( R[[X]] \) is the set of sequences \( \{a_n\} \) in \( R \) written \( a_0 + a_1X + a_2X^2 + ... \) [7]. The ring \( R((X)) \) is the ring of formal Laurent series over \( R \). A formal Laurent series is defined as a power series with finitely many terms of negative degree.
**Definition 1.1** Let \( R \) be a ring and \( F = \sum_{i=0}^{n} \alpha_i Y^{n-i} \) be an element of \( R[[X]][Y] \). Each \( \alpha_i \) is a formal power series \( \sum \alpha_i(j) X^j \). Then \( F \neq 0 \), read \( F \) apart from 0, iff the ideal generated by all \( \alpha_i(j) \) contains 1. We write \( F \not\equiv G \) to mean \( F - G \not\equiv 0 \). If \( R \) is a field, or even a local ring, this is equivalent to say that there exist \( i \) and \( j \) such that \( \alpha_i(j) \) is invertible.

In this section, we only need this notion in the case where \( R \) is a field. But even in this case, the definition in terms of ideals is convenient to prove in a constructive framework basic properties of apartness.

If \( F \) is in \( R[[X]][Y] \) we let \( F_Y \) be the derivative of \( F \) with respect to \( Y \).

**Lemma 1.2** Let \( R \) be a ring and let \( F \in R[[X]][Y] \). If there exist \( P, Q \in R[[X]][Y] \) and \( \gamma \neq 0 \) in \( R[[X]] \) such that \( PF + QF_Y = \gamma \), then \( \forall n > 1 \) \( F \not\equiv Y^n \).

**Proof** Let \( n > 1 \) and let \( G = F - Y^n \) then \( PG + QG_Y \) is of the form \( \gamma + YH \) for some \( H \) in \( R[[X]][Y] \) and hence \( PG + QG_Y \not\equiv 0 \). Since all coefficients of \( PG + QG_Y \) are in the ideal generated by the coefficients of \( G \) we have \( G \not\equiv 0 \).

**Lemma 1.3** Let \( R \) be a ring containing \( \mathbb{Q} \). Let \( f = Y^n + \sum_{i=1}^{n} c_i Y^{n-i} \in R[Y] \) be a monic polynomial of degree \( n \). If \( c_1 = 0 \) and some coefficient \( c_m \) is a unit, then \( \forall a \in R f \not\equiv (Y - a)^n \).

**Proof** Indeed \( c_m \) belongs to the ideal generated by the coefficients of \( f - (Y - a)^n \).

One key of Abhyankar’s proof is Hensel’s Lemma. We formulate a little more general version than the one in [1].

**Lemma 1.4** (Hensel’s Lemma) Let \( R \) be a ring and \( F(X, Y) = Y^n + \sum_{i=1}^{n} a_i(X) Y^{n-i} \) be a monic polynomial in \( R[[X]][Y] \) of degree \( n > 1 \). Given monic \( G_0, H_0 \in R[Y] \) of degrees \( r, s > 0 \) respectively and \( H^*, G^* \in R[Y] \) such that \( F(0, Y) = G_0H_0 \), \( r + s = n \) and \( G_0H^* + H_0G^* = 1 \); we can find \( G(X, Y), H(X, Y) \in R[[X]][Y] \) of degrees \( r, s \) respectively, such that \( F(X, Y) = G(X, Y)H(X, Y) \) and \( G(0, Y) = G_0, H(0, Y) = H_0 \).

**Proof** The proof is almost the same as Abhyankar’s [1], we present it here for completeness.

Since \( R[[X]][Y] \subseteq R[Y][[X]] \), we can rewrite \( F(X, Y) \) as a power series in \( X \) with coefficients in \( R[Y] \). Let \( F(X, Y) = F_0(Y) + F_1(Y)X + \ldots + F_q(Y)X^q + \ldots \), with \( F_i(Y) \in R[Y] \). Now we want to find \( G(X, Y), H(X, Y) \in R[Y][[X]] \) such that \( F = GH \). If we let
Let \( G = G_0 + \sum_{i=1}^{\infty} G_i(Y)X^i \) and \( H = H_0 + \sum_{i=1}^{\infty} H_i(Y)X^i \), then for each \( q \) we need to find \( G_i(Y), H_j(Y) \) for \( i, j \leq q \) such that \( F_q = \sum_{i+j=q} G_iH_j \). We also need \( \deg G_k < r \) and \( \deg G_t < s \) for \( k, t > 0 \).

We find \( G_i, H_j \) by induction on \( q \). We have that \( F_0 = G_0H_0 \). Assume that for some \( q > 0 \) we have found all \( G_i, H_j \) with \( \deg G_i < r \) and \( \deg H_j < s \) for \( 1 \leq i < q \) and \( 1 \leq j < q \). Now we need to find \( H_q, G_q \) such that

\[
F_q = G_0H_q + H_0G_q + \sum_{i+j=q \atop i < q, j < q} G_iH_j.
\]

We let \( U_q = F_q - \sum_{i+j=q \atop i < q, j < q} G_iH_j \), and we can see that \( \deg U_q < n \). We are given that \( G_0H^* + H_0G^* = 1 \). Multiplying by \( U_q \) we get \( G_0H^*U_q + H_0G^*U_q = U_q \). By Euclidean division we can write \( U_qH^* = E_qH_0 + H_q \) for some \( E_q, H_q \) with \( \deg H_q < s \). Thus we write \( U_q = G_0H_q + H_0(E_qG_0 + G^*U_q) \).

We can see that \( \deg H_0(E_qG_0 + G^*U_q) < n \) since \( \deg(U_q - G_0H_q) < n \). Since \( H_0 \) is monic of degree \( s \), \( \deg(E_qG_0 + G^*U_q) < r \). We take \( G_q = E_qG_0 + G^*U_q \).

Now, we can write \( G(X, Y), H(X, Y) \) as monic polynomials in \( Y \) with coefficients in \( R[[X]] \), with degrees \( r, s \) respectively.

If \( \alpha = \sum \alpha(i)X^i \) is an element of \( R[[X]] \) we write \( m \leq \text{ord} \alpha \) to mean that \( \alpha(i) = 0 \) for \( i < m \) and \( m = \text{ord} \alpha \) to mean furthermore that \( \alpha(m) \) is invertible.

**Lemma 1.5** Let \( K \) be an algebraically closed field of characteristic zero.

Let \( F(X, Y) = Y^n + \sum_{i=1}^{n} \alpha_i(X)Y^{n-1} \in K[[X]][[Y]] \) be a monic non-constant polynomial such that \( PF + QFY = \gamma \) for some \( P, Q \in K[[X]][[Y]] \) and \( \gamma \neq 0 \) in \( K[[X]] \). Then there exist \( m > 0 \) and a proper factorization \( F(T^m, Y) = G(T, Y)H(T, Y) \) with \( G \) and \( H \) in \( K[[X]][[Y]] \).

**Proof** We can assume w.l.o.g. that \( \alpha_1(X) = 0 \). (This is Shreedharacharya’s\(^2\) trick \cite{1}.)

The simple case is if we have \( \text{ord} \alpha_i = 0 \) for some \( i \). For any root \( b \) of \( F(0, b) = 0 \) we have then by Lemma 1.3 a proper decomposition \( F(0, Y) = (Y - b)^pH \) with \( Y - b \) and \( H \) coprime, and we can use Hensel’s Lemma to conclude (In this case we can take \( m = 1 \).)

In general, we know by Lemma 1.2 that some \( \alpha_k(X) \) is apart from 0. We then have \( \alpha_k(\ell) \) invertible for some \( \ell \). We can then find \( m \) and \( p \) such that \( \alpha_m(p) \) is invertible and \( \alpha_j(0) = 0 \) whenever \( j/i < p/m \). We can then write

\[
F(T^m, T^rZ) = T^{rp}(Z^n + c_2(T)Z^{n-2} + \cdots + c_n(T))
\]

with \( \text{ord} c_m = 0 \). As in the simple case, we have a proper decomposition \( Z^n + c_2(T)Z^{n-2} + \cdots + c_n(T) = G_1(T, Z)H_1(T, Z) \) with \( G_1(T, Z) \) monic of degree \( l \) in \( Z \)

\(^2\)Shreedharacharya’s trick is also known as Tschirnhaus’s trick.
and $H_1(T,Z)$ monic of degree $q$ in $Z$, with $l + q = n$, $l < n$, $q < n$. We then take $G(T,Y) = T^{lp}G_1(T,Y/T^p)$ and $H(T,Y) = T^{qp}H_1(T,Y/T^p)$.

We note that since the polynomial is of finite $Y$ degree the search for $m$ and $p$ is finite. For example if the polynomial is of $Y$ degree 7 (see Figure 1) and if $k = 4$ and $\ell = 3$ we need only search the finite number of pairs inside the polygon edges (The dashed lines in the figure).

![Newton Polygon](image)

**Figure 1: Newton Polygon**

**Theorem 1.6** Let $K$ be an algebraically closed field of characteristic zero. Let $F(X,Y) = Y^n + \sum_{i=1}^{n} \alpha_i(X) Y^{n-i} \in K[[X]][Y]$ be a monic non-constant polynomial such that $PF + QF_Y = \gamma$ for some $P, Q \in K[[X]][Y]$ and $\gamma \neq 0$ in $K[[X]]$. Then there exist a positive integer $m$ and factorization

$$F(T^m, Y) = \prod_{i=1}^{n_1} (Y - \eta_i) \quad \eta_i \in K[[T]]$$

**Proof** This follows directly from Lemma 1.5, since for any factor $G$ of $F$ we can find $S, T \in K[[X]][Y]$, $\beta \in K[[X]]$ with $\beta \neq 0$ such that $SG + TG_Y = \beta$.

**Corollary 1.7** Let $K$ be an algebraically closed field of characteristic zero. The field of fractional power series over $K$ is separably algebraically closed.
The same strategy can be used to show that the field of fractional power series over a real closed field is separably real closed.

2 Dynamical interpretation

The goal of this section is to give a version of Theorem 1.6 over a discrete field $K$ of characteristic 0, not necessarily algebraically closed.

Definition 2.1 (Regular ring) A commutative ring $R$ is (von Neumann) regular if for every element $a \in R$ there exist $b \in R$ such that $aba = a$ and $bab = b$. This element $b$ is called the quasi-inverse of $a$.

A ring is regular iff it is zero-dimensional and reduced. It is also equivalent to the fact that any principal ideal (and hence any finitely generated ideal) is generated by an idempotent. If $a$ is an element in $R$ and $aba = a$, $bab = b$ then the element $e = ab$ is an idempotent such that $\langle e \rangle = \langle a \rangle$ and $R$ is isomorphic to $R_0 \times R_1$ with $R_0 = R/\langle e \rangle$ and $R_1 = R/(1 - e)$. Furthermore $a$ is 0 on the component $R_0$ and invertible on the component $R_1$.

We define strict Bézout rings as in [6, Ch 4].

Definition 2.2 A ring $R$ is a (strict) Bézout ring if for all $a, b \in R$ we can find $g, a_1, b_1, c, d \in R$ such that $a = a_1g$, $b = b_1g$ and $ca_1 + db_1 = 1$.

If $R$ is a regular ring then $R[X]$ is a strict Bézout ring (and the converse if true [6]).

Intuitively we can compute the gcd as if $R$ was a field, but we may need to split $R$ when deciding if an element is invertible or 0. Using this, we see that given $a, b$ in $R[X]$ we can find a decomposition $R_1, \ldots, R_n$ of $R$ and for each $i$ we have $g, a_1, b_1, c, d$ in $R_i[X]$ such that $a = a_1g$, $b = b_1g$ and $ca_1 + db_1 = 1$ with $g$ monic. The degree of $g$ may depend on $i$.

Definition 2.3 (Separable polynomial) Let $R$ be a ring. A polynomial $p \in R[X]$ is separable if there exist $r, s \in R[X]$ such that $rp + sp' = 1$, where $p' \in R[X]$ is the derivative of $p$.

Lemma 2.4 If $R$ is regular and $p$ in $R[X]$ is a separable polynomial then $R[a] = R[X]/\langle p \rangle$ is regular.
We show that $a = \gcd(f)$ which is the gcd of $A$. This implies that $h = X^n - f = X^n - g^p$ is a unit.

The following result is usually proved with the assumption of existence of a decomposition into irreducible factors. We give a proof without this assumption (It works over any characteristic).

**Lemma 2.5** Let $f$ be a monic polynomial in $K[X]$ where $K$ is a field. If $f'$ is the derivative of $f$ and $g$ monic is the gcd of $f$ and $f'$ then writing $f = hg$ we have that $h$ is separable. We call $h$ the separable associate of $f$.

**Proof** Let $a$ be the gcd of $h$ and $h'$. We have $h = l_1a$. Let $d$ be the gcd of $a$ and $a'$. We have $a = l_2d$ and $a' = m_2d$, with $l_2$ and $m_2$ coprime.

The polynomial $a$ divides $h' = l_1a' + l'_1a$ and hence that $a = l_2d$ divides $l_1a' = l_1m_2d$. It follows that $l_2$ divides $l_1m_2$ and since $l_2$ and $m_2$ are coprime, that $l_2$ divides $l_1$.

Also, if $a^n$ divides $p$ then $p = qa^n$ and $p' = q'a^n + nqa'a^{n-1}$. Hence $da^{n-1}$ divides $p'$. Since $l_2$ divides $l_1$, this implies that $a^n = l_2da^{n-1}$ divides $l_1p'$. So $a^{n+1}$ divides $al_1p' = hp'$.

We show that $a^n$ divides $g$ for all $n$ by induction on $n$. If $a^n$ divides $g$ we have just seen that $a^{n+1}$ divides $g'h$. Also $a^{n+1}$ divides $h'g$ since $a$ divides $h'$. So $a^{n+1}$ divides $g'h + h'g = f'$. On the other hand, $a^{n+1}$ divides $f = hg = l_1ag$. So $a^{n+1}$ divides $g$ which is the gcd of $f$ and $f'$.

This implies that $a$ is a unit. 

**A triangular separable $K$-algebra**

$$R = K[a_1, \ldots, a_n], \ p_1(a_1) = 0, \ p_2(a_1, a_2) = 0, \ldots$$

is a sequence of separable extension starting from a discrete field $K$, with $p_1$ in $K[X]$, $p_2$ in $K[a_1][X], \ldots$ all monic and separable polynomials. A triangular separable algebra is thought of as an approximation of the algebraic closure of $K$, and is determined by a list of polynomials $p_1(X_1), p_2(X_1, X_2), \ldots$ (This is related to the way [5] avoids the algebraic closure, by adding only constants as needed, with the difference that we don’t assume an irreducibility test.) It follows from Lemma 2.4 that each triangular separable algebra defines a regular algebra $K[a_1, \ldots, a_n]$. In this case however, the
idempotent elements have a simpler direct description. If we have a decomposition
\( p_1(a_1, \ldots, a_{l-1}, X) = g(X)q(X) \) with \( g, q \) in \( K[a_1, \ldots, a_{l-1}, X] \) then since \( p_1 \) is separable, we have a relation \( rg + sq = 1 \) and \( e = r(a_i)g(a_i) \), \( 1 - e = s(a_i)g(a_i) \) are then
idempotent element. We then have a decomposition of \( R \) in two triangular separable
algebras \( p_1, \ldots, p_{l-1}, g, p_{l+1}, \ldots \) and \( p_1, \ldots, p_{l-1}, q, p_{l+1}, \ldots \). If we iterate this process
we obtain the notion of decomposition of a triangular separable algebra \( R \) in finitely
many triangular algebra \( R_1, \ldots, R_n \). This decomposition stops when all polynomials
\( p_1, \ldots, p_l \) are irreducible, i.e. when \( R \) is a field. For a triangular separable algebra \( R \)
and an ideal \( I \) of \( R \), if \( R/I \) is a triangular separable algebra then we describe \( R/I \) as
being a refinement of \( R \). Thus a refinement of \( K[a_1, \ldots, a_n], p_1, \ldots, p_n \) is of the form
\( K[b_1, \ldots, b_n], q_1, \ldots, q_n \) with \( q_i \mid p_i \).

The following is a corollary of Lemma 2.5

**Corollary 2.6** Let \( f \) be a monic polynomial in \( R[X] \) where \( R \) is a triangular separable
\( K \)-algebra. If \( f' \) is the derivative of \( f \) then there exist a decomposition \( R_1, \ldots, R_n \) and
on each \( R_i \) we can find polynomials \( h, g, q, r, s \) in \( R_i[X] \) such that \( f = hg, f' = qg \) and
\( rh + sq = 1 \) with \( h \) monic and separable.

Lemma 1.5 becomes in this way.

**Lemma 2.7** Let \( R \) be a triangular separable algebra over a field \( K \) of characteristic 0.
Let \( F(X, Y) = Y^n + \sum_{i=1}^{n} \alpha_i(X)Y^{n-i} \in R[[X]][Y] \) be a monic non-constant polynomial
such that \( PF + QF_Y = \gamma \) for some \( P, Q \in R[[X]][Y] \) and \( \gamma \neq 0 \) in \( R[[X]] \).
There exists then a decomposition \( R_1, \ldots, R_m \) of \( R \) and for each \( i \) there exist \( m > 0 \) and a
proper factorization \( F(T^m, Y) = G(T, Y)H(T, Y) \) with \( G \) and \( H \) in \( S_i[[T]][Y] \) where
\( S_i = R_i[a] \) is a separable extension of \( R_i \).

**Proof** The proof proceeds as the proof of Lemma 1.5, assuming w.l.o.g. \( \alpha_1 = 0 \). We first find a decomposition \( R_1, \ldots, R_m \) of \( R \) and for each \( l \) we can then find \( m \) and \( p \) such that
\( \alpha_m(p) \) is invertible and \( \alpha_j(j)/0 \) whenever \( j/i < p/m \) in \( R_i \). We can then write
\[
F(T^m, T^p Z) = T^{\alpha_p}(Z^n + c_2(T)Z^{n-2} + \cdots + c_n(T))
\]
with \( c_m = 0 \). We then find a further decomposition \( R_{l1}, R_{l2}, \ldots \) of \( R_i \) and for each
\( q \) a number \( s \) and a separable extension \( R_{lq}[a] \) of \( R_{lq} \) such that
\[
Z^n + c_2(0)Z^{n-2} + \cdots + c_n(0) = (Z - a)^sL(Z)
\]
with \( L(a) \) invertible. Using Hensel’s Lemma, we can lift this to a proper decomposition
\( Z^n + c_2(T)Z^{n-2} + \cdots + c_n(T) = G_1(T, Z)H_1(T, Z) \) with \( G_1(T, Z) \) monic of degree \( t \)
and \( H_1(T, Z) \) monic of degree \( u \). We take \( G(T, Y) = T^{\alpha_p}G_1(T, Y/T^p) \) and \( H(T, Y) = T^{\alpha_p}H_1(T, Y/T^p) \).
We can then state the following version of Newton-Puiseux algorithm.

**Theorem 2.8** Let $K$ be a field of characteristic 0. Let $F(X, Y) = Y^n + \sum_{i=1}^n \alpha_i(X)Y^{n-i}$ in $K[[X]][Y]$ be a monic non-constant polynomial such that $PF + QFY = \gamma$ for some $P, Q \in K[[X]][Y]$ and $\gamma \neq 0$ in $K[[X]]$. There exists then a triangular separable algebra $R$ over $K$ and $m > 0$ and a factorization

$$F(T^m, Y) = \prod_{i=1}^{\eta_1} (Y - \eta_i) \quad \eta_i \in R[[T]]$$

The algorithm for computing this factorization proceeds by induction on $n$, using Lemma 2.7. More precisely the algorithm proceeds as follows. At a given point, we have computed

1. a triangular separable extension $R$ of $K$
2. a number $m$ and a partial decomposition $F(T^m, Y) = H_1(T, Y) \ldots H_r(T, Y)$ with all $H_i \in R[[T]][Y]$ monic in $Y$.

The algorithm stops if all $H_i$ are of degree 1 in $Y$. Otherwise, we apply Lemma 2.7 to the first polynomial $H_i(T, Y)$ of degree $> 1$ in $Y$ to compute a decomposition of $R$ and for each algebra $S$ in this decomposition a number $p$ and a proper decomposition $H_i(T^p, Y) = G(T, Y)G_1(T, Y)$. We select then one algebra, and we proceed with the decomposition

$$F(T^{mp}, Y) = H_1(T^p, Y) \ldots H_{i-1}(T^p, Y)G(T, Y)G_1(T, Y)H_{i+1}(T^p, Y) \ldots H_r(T^p, Y)$$

### 3 Analysis of the theorem

The previous algorithm is not deterministic. The goal of this section is to compare two possible triangular separable algebras that can be obtained by this algorithm. We are going to show that they are both powers of a common triangular algebra.

In the following we refer to the elementary symmetric polynomials in $n$ variables by $\sigma_1, \ldots, \sigma_n$ taking $\sigma_j(X_1, \ldots, X_n) = \sum_{1 \leq j_1 < \ldots < j_l \leq n} X_{j_1} \ldots X_{j_l}$.

**Lemma 3.1** Let $R$ be a reduced ring. Given $a_1, \ldots, a_n \in R$, if $\sigma_j(a_1, \ldots, a_n) = 0$ for $0 < i \leq n$ then $a_1 = a_2 = \ldots = a_n = 0$.

**Proof** We have $\prod_{i=1}^n (X - a_i) = X^n$. Hence, $a_i^j = 0$ for $0 < i \leq n$ and since $R$ is reduced, $a_i = 0$. \qed
Lemma 3.2  Let \( R \) be a reduced ring. Given \( \alpha_1, \ldots, \alpha_n \in R[[X]] \) such that for some positive rational number \( d \) we have \( \text{ord}(\sigma_i(\alpha_1, \ldots, \alpha_n)) \geq di \) for \( 0 < i \leq n \). Then \( \text{ord}(\alpha_i) \geq d \) for \( 0 < i < n \).

**Proof**  Let \( \alpha_i = \sum_{j=1}^{\infty} \alpha_i(j)X^j \). We show that \( \alpha_i(j) = 0 \) if \( j < d \). Assume that we have \( \alpha_i(j) \neq 0 \) for \( j < m < d \). We show then \( \alpha_i(m) = 0 \) for \( i = 1, \ldots, n \). The coefficient of \( X^m \) in \( \sigma_i(\alpha_1, \ldots, \alpha_n) \) is \( \sigma_i(\alpha_1(m), \ldots, \alpha_n(m)) \). Since \( \text{ord}(\sigma_i(\alpha_1, \ldots, \alpha_n)) > mi \) we get that \( \sigma_i(\alpha_1(m), \ldots, \alpha_n(m)) = 0 \) and hence by Lemma 3.1 we get that \( \alpha_i(m) = 0 \) for \( i = 1, \ldots, n \). \( \square \)

Lemma 3.3  For a ring \( R \) and a reduced extension \( R \to A \), let \( F = Y^n + \sum_{i=1}^{n} \alpha_i Y^{n-i} \) be an element of \( R[[X]][Y] \) such that \( F(T^q, T^pZ) = T^p F(T, Z) \) with \( F_1 \) in \( R[[T]][Z] \) for some \( q > 0, p \). If \( F(U^m, Y) \) factors linearly over \( A[[U]] \) for some \( m > 0 \) then \( F_1(0, Z) \) factors linearly over \( A \).

**Proof**  We have \( F(U^m, Y) = \prod_{i=1}^{n} (Y - \eta_i), \eta_i \in A[[U]] \) and hence we have \( F(V^m, V^pZ) = \prod_{i=1}^{n} (V^p Z - \eta_i(V^q)), \eta_i(U) \in A[[U]] \) and

\[
F_1(V^m, Z) = \prod_{i=1}^{n} (Z - V^{-mp} \eta_i(V^q)) = Z^n + \sum_{i=1}^{n} V^{-mp} \beta_i(V^q) Z^{n-i}
\]

Since \( F_1(T, Z) \) is in \( R[[T]][Z] \) we have \( mp \leq \text{ord} \beta_i(V^q) \).

Since \( \beta_i(V^q) = \sigma_i(\eta_1(V^q), \ldots, \eta_n(V^q)) \), Lemma 3.2 shows that \( mp \leq \text{ord} \eta_i(V^q) \) for \( 0 < i < n \). Hence \( \mu_i(V) = V^{-mp} \eta_i(V^q) \) is in \( A[[V]] \) and since \( F_1(V, Z) = \prod_{i=1}^{n} (Z - \mu_i(V)) \), we have that \( F_1(0, Z) \) factors linearly over \( A \), of roots \( \mu_i(0) \). \( \square \)

Definition 3.4  Let \( R = K[a_1, \ldots, a_n], p_1, \ldots, p_n \) be a triangular separable algebra with \( p_i \) of degree \( m_i \) and \( A \) an algebra over \( K \). Then \( A \) splits \( R \) if there exist a family of elements \( \{a_{i_1, \ldots, i_l} \in A \mid 0 < l \leq n, 0 < i_j \leq m_j \} \) such that

\[
p_1 = \prod_{d=0}^{m_1} (X - a_d)
\]

\[
p_{l+1}(a_{i_1}, a_{i_1, i_2}, \ldots, a_{i_1, \ldots, i_l}, X) = \prod_{d=0}^{m_{l+1}} (X - a_{i_1, \ldots, i_l, d})
\]

for \( 0 < l < n \)

We can view the previous definition as that of a tree of homomorphisms from the subalgebras of \( R \) to \( A \) at the root we have the identity homomorphism from \( K \) to \( A \).
We note that if an algebra \( A \) we have \((\text{since } p_g \bar{a} \text{ is a monic non-constant polynomial of degree } n)\). From this we obtain \( m_1 \) homomorphisms \( \varphi_1, ..., \varphi_{m_1} \) from \( K[a_1] \) to \( A \) each taking \( a_1 \) to a different \( \bar{a}_{ij} \). If \( p_2 \) factors linearly under say \( \varphi_1 \), i.e. \( \varphi_1(p_2) = \prod_{j=0}^{m_2} (X - \bar{a}_{2j}) \) then we obtain \( m_2 \) different (since \( p_2 \) is separable) homomorphisms \( \varphi_{11}, ..., \varphi_{1m_2} \) from \( K[a_1, a_2] \) to \( A \). Similarly we obtain \( m_2 \) different homomorphisms from \( K[a_1, a_2] \) to \( A \) by extending \( \varphi_2, \varphi_3, ... \) etc, thus having \( m_1m_2 \) homomorphism in total. Continuing in this fashion we obtain the \( m \) different homomorphisms of the family \( S \).

We note that if an algebra \( A \) over \( K \) splits a triangular separable algebra \( R \) over \( K \) then \( A \otimes_K R \cong A^{[R:K]} \). If \( A \) is a field then the converse is also true as the following lemma shows.

**Lemma 3.5** Let \( L/K \) be a field and \( R = K[a_1, ..., a_n], p_1, ..., p_n \) a triangular separable algebra. Then \( L \otimes_K R \cong L^{[R:K]} \) only if \( L \) splits \( R \).

**Proof** Let \( \deg(p_i) = m_i, [R : K] = m = \prod_{i=1}^n m_i \) and let \( L \otimes_K R \cong L^{[R:K]} \). Then there exist a system of orthogonal idempotents\(^3\) \( e_1, ..., e_m \) such that \( A = L \otimes_K R \cong A/(1 - e_1) \times ... \times A/(1 - e_m) = L^m \). Let \( a_{ij} \) be the image of \( a_i \) in \( A/(1 - e_j) \). Then we have \( (a_{11}, ..., a_{n1}) \neq (a_{12}, ..., a_{n2}) \neq ... \neq (a_{1m}, ..., a_{nm}) \) since otherwise we will have the ideals \( (1 - e_i) = (1 - e_j) \) for some \( i \neq j \). Since \( p_1 \) is separable there are up to \( m_1 \) different images \( a_{ij} \) of \( a_1 \). Thus the size of the set \( \{a_{ij} \mid 0 < j \leq m\} \) is equal to \( m_1 \) only if \( p_1 \) factors linearly over \( L \). Similarly, for each different image \( \bar{a}_1 \) of \( a_1 \) there are up to \( m_2 \) possible images of \( \bar{a}_2 \) in \( L \) since the polynomial \( p_2(\bar{a}_2, X) \) is separable. Thus the size of the set \( \{(a_{1j}, a_{2j}) \mid 0 < j \leq m\} \) is equal \( m_1m_2 \) only if \( p_1 \) factors linearly over \( L \) and for each root \( \bar{a}_1 \) of \( p_1 \) the polynomial \( p_2(\bar{a}_1, X) \) factors linearly over \( L \). Continuing in this fashion we find that the size of the set \( \{(a_{ij}, ..., a_{nj}) \mid 0 < j \leq m\} \) is equal to \( m_1...m_n = m \) only if \( L \) splits \( R \). \( \Box \)

**Lemma 3.6** Let \( A \) be a triangular separable algebra over a field \( K \) and let \( p \) be a monic non-constant polynomial of degree \( m \) in \( A[X] \) such that \( p = \prod_{i=1}^m (X - a_i) \) with \( a_i \in A \). If \( g \) is a monic non-constant polynomial of degree \( n \) such that \( g \mid p \) then we have a decomposition \( A \cong R_1 \times ... \times R_t \) such that for any \( R_j \) in the product \( g = \prod_{i=1}^n (X - \bar{a}_i) \) with \( \bar{a}_i \in R_j \) the image in \( R_j \) of some \( a_k, 0 < k \leq m \).

**Proof** Let \( p = (X - a_1)...(X - a_n) \) for \( a_1, ..., a_n \in A \). Let \( p = gq \). Then \( p(a_i) = g(a_i)q(a_i) = 0 \). We can find a decomposition of \( A \) into triangular separable algebras \( A_1 \times ... \times A_t \times B_1 \times B_s \) such that \( g(a_i) = 0 \) in \( A_i, 0 < i \leq t \) and \( g(a_1) \) is a unit in

\(^3\)That is \( e_ie_j = 0 \) if \( i \neq j \) and \( e_1 + ... + e_m = 1 \)
Let \( R \in \mathcal{R}_B \) be a triangular separable algebra over \( K \) such that \( A \) splits \( R \). Let \( B \) be a refinement of \( R \). Then we can find a decomposition \( A \cong A_1 \times \ldots \times A_n \) into a product of triangular separable algebras such that \( A_i \) splits \( B \) for \( 0 < i \leq m \).

**Proof** Let \( R = K[a_1, \ldots, a_n], p_1, \ldots, p_n \). Then \( B = K[\bar{a}_1, \ldots, \bar{a}_n], g_1, \ldots, g_n \) where \( g_j \mid p_j \) for \( 0 < j \leq n \). Let \( \deg(p_j) = m_j \) and \( \deg(g_j) = \ell_j \) for \( 0 < j \leq n \). Since \( A \) splits \( R \), we have a family of elements \( \{a_{ij} \mid a_{ij} \in A \times \ldots \times A_{m_i} \} \) satisfying the conditions of Definition 3.4. We claim that the family \( \{a_{ij} \mid a_{ij} \in A \times \ldots \times A_{m_i} \} \) splits \( B \) over \( A \). Continuing in this fashion we can find a decomposition of \( A \) such that each algebra in the decomposition splits \( B \).

**Lemma 3.8** Let \( A \) and \( B \) be triangular separable algebras such that \( A \cong A_1 \times \ldots \times A_t \) and each \( A_i \) splits \( B \). Then \( A \) splits \( B \).

**Proof** Let \( B = K[a_1, \ldots, a_n], g_1, \ldots, g_n \) with \( \deg(g_i) = m_i \). Then we have a family of elements \( \{a_{ki} \mid 0 < k_j \leq m_j, 0 < j \leq n \} \) in \( A_i \) satisfying the conditions of Definition 3.4. We claim that the family

\[
S = \{a_{ki} \mid a_{ki} \in (a_{k1}, \ldots, a_{kt}), 0 < k_j \leq m_j, 0 < j \leq n\}
\]

of \( A \) elements satisfy the conditions of Definition 3.4. Since we have a factorization

\[

\prod_{l=1}^{m_1} (X - a_{l}) \quad \text{over } A_i,
\]

we have a factorization

\[

g_1 = \prod_{l=1}^{m_1} (X - a_{l}) \quad \text{over } A_i,
\]

we have a factorization

\[

g_1 = \prod_{l=1}^{m_1} (X - (a_{l}, \ldots, a_{t})) \quad \text{over } A.
\]

Since \( 0 < l \leq m_1 \) we have a factorization

\[

g_2(a_{l}, X) = \prod_{j=1}^{m_2} (X - a_{lj}) \quad \text{in } A_i,
\]

we have a factorization

\[

g_2(a_{l}, X) = \prod_{j=1}^{m_2} (X - (a_{l}, \ldots, a_{t})) \quad \text{over } A.
\]

Continuing in this fashion we verify that the family \( S \) satisfy the requirements of Definition 3.4.
Corollary 3.9  Let $A$ and $B$ be triangular separable algebras such that $A$ splits $B$. Then $A$ splits any refinement of $B$.

Lemmas 3.3, 3.8 and Corollary 3.9 allow us to extend Lemma 2.7 as follows

Lemma 3.10  Let $R = K[a_1,\ldots,a_n], p_1,\ldots,p_n$ be a triangular separable algebra with $\text{deg}(p_i) = m_i$. Let $F(a_1,\ldots,a_n, X, Y) = Y^n + \sum_{i=1}^n a_i(X)Y^{n-i} \in R[[X]][Y]$ be a monic non-constant polynomial such that $PF + QF_Y = \gamma$ for some $P, Q \in R[[X]][Y], \gamma \in R[[X]]$ with $\gamma \neq 0$. There exists then a decomposition $R_1,\ldots,$ of $R$ and for each $i$ there exist $m > 0$ and a proper factorization $F(T^m, Y) = G(T, Y)H(T, Y)$ with $G$ and $H$ in $S_i[[T]][Y]$ where $S_i = R_i[b], q$ is a separable extension of $R_i$.

Moreover, Let $A$ be a triangular separable algebra such that $A$ splits $R$ and let $\{a_{i_1,\ldots,i_n} | 0 < l \leq n, 0 < i \leq m_i \}$ be the family of elements in $A$ satisfying the conditions in Definition 3.4. If $F(a_{i_1,\ldots,i_n}, X, Y)$ factors linearly over $A[[U]]$ for $0 < i \leq m_i$ where $U^n = X$ for some positive integer $v$ then $A$ splits $S_i$.

Proof  The proof proceeds as the proof of Lemma 1.5, assuming w.l.o.g. $\alpha_1 = 0$. We first find a decomposition $R_1,\ldots,$ of $R$ and for each $l$ we can then find $m$ and $p$ such that $\alpha_m(p)$ is invertible and $\alpha_i(j) = 0$ whenever $j/i < p/m$ in $R_l$. We can then write

$$F(T^m, T^lZ) = T^{mpl}(Z^n + c_2(T)Z^{n-2} + \cdots + c_n(T))$$

with $c_m = 0$. Since $A$ splits $R$ then by Lemma3.7 we can find a decomposition $A_1,\ldots,$ of $A$ such that each $A_l$ splits $R_l$ for each $l$. Then each $A_l$ can be decomposed into $A_{l_1,\ldots,l_s},$ where each $A_{l_1,\ldots,l_s}$ is a separable extension of $A_{l_1,\ldots,l_s-1}$ and for each $s$ a separable extension $R_{l_t}[a]$ of $R_{l_t}$ such that

$$q = Z^n + c_2(0)Z^{n-2} + \cdots + c_n(0) = (Z - a)^sL(Z)$$

with $L(a)$ invertible. Similarly, we can decompose each $A_l$ further into $B_1,\ldots,$ such that each $B_l$ splits each $R_{l_t}$ for all $l, t$. Let the family $F = \{b_{i_1,\ldots,i_n} | 0 < l \leq m, 0 < i \leq m_i \}$ be the image of the family $\{a_{i_1,\ldots,i_n} | 0 < l \leq n, 0 < i \leq m_i \}$ in $B_l$. Then each $B_l$ splits $R$ with $F$ as the family of elements of $B_l$ satisfying Definition 3.4. But then $F(b_{i_1,\ldots,i_n}, X, Y)$ factors linearly over $B_l$. For some subfamily $\{c_{i_1,\ldots,i_n} | 0 < l \leq n, 0 < i_j \leq m_j \} \subset F$ of elements in $B_l$ we have that $B_l$ splits $R_{l_n}$. Thus $F(c_{i_1,\ldots,i_n}, X, Y)$ factors linearly over $B_l$ for all $c_{i_1,\ldots,i_n}$ in the family. By Lemma 3.3 we have that $q(c_{i_1,\ldots,i_n}, Z)$ factors linearly over $B_l$ for all $c_{i_1,\ldots,i_n}$. Thus $B_l$ splits the extension $R_{l_n}[a]$. But then by Lemma 3.8 we have that $A$ splits $R_{l_n}[a]$. Using Hensel’s Lemma, we can lift this to a proper decomposition $Z^n + c_2(T)Z^{n-2} + \cdots + c_n(T) = G_1(T, Z)H_1(T, Z)$ with $G_1(T, Z)$ monic of degree $t$ and $H_1(T, Z)$ monic of degree $u$. We take $G(T, Y) = T^{mp}G_1(T, Y/T^p)$ and $H(T, Y) = T^{mp}H_1(T, Y/T^p)$.
We can then extend Theorem 2.8 as follows.

**Theorem 3.11** Let \( F(X, Y) = Y^n + \sum_{i=1}^n \alpha_i(X)Y^{n-i} \in K[[X]][Y] \) be a monic non-constant polynomial such that \( PF + QF_Y = \gamma \) for some \( F, P, Q \in K[[X]][Y], \gamma \in K[[X]] \) with \( \gamma \neq 0 \). There exists then a triangular separable algebra \( R \) over \( K \) and \( m > 0 \) and a factorization

\[
F(T^m, Y) = \prod_{i=1}^{n_1} (Y - \eta_i) \quad \eta_i \in R[[T]]
\]

Moreover, if \( A \) is a triangular separable algebra over \( K \) such that \( F(X, Y) \) factors linearly over \( A[[X^{1/s}]] \) for some positive integer \( s \) then \( A \) splits \( R \).

As we shall see in the examples below, the result of the computation is usually several triangular separable algebras \( R_1, \ldots \) over the base field \( K \) with linear factorizations of \( F \) over \( R_i[[X^{1/r}]] \), ... for some \( r \in \mathbb{Z}^+ \). The previous theorem allows us to state the following about these algebras.

**Corollary 3.12** Let \( A \) and \( B \) be two triangular separable algebras obtained by the algorithm of Theorem 2.8. Then \( A \) splits \( B \) and \( B \) splits \( A \). Consequently, a triangular separable algebra obtained by this algorithm splits itself.

Thus given any two algebras \( R_1 \) and \( R_2 \) obtained by the algorithm and two prime ideals \( P_1 \in \text{Spec}(R_1) \) and \( P_2 \in \text{Spec}(R_2) \) we have a field isomorphism \( R_1/P_1 \cong R_2/P_2 \). Therefore all the algebras obtained are approximations of the same field \( L \). Since \( L \) splits all the algebras and itself is a refinement, \( L \) splits itself, i.e. \( L \otimes_K L \cong L^{[L:K]} \) and \( L \) is a normal, in fact a Galois extension of \( K \).

Classically, this field \( L \) is the field of constants generated over \( K \) by the set of coefficients of the Puiseux expansions of \( F \). The set of Puiseux expansions of \( F \) is closed under the action of \( \text{Gal}(\bar{K}/K) \), where \( \bar{K} \) is the algebraic closure of \( K \). Thus the field of constants generated by the coefficients of the expansions of \( F \) is a Galois extension. The algebras generated by our algorithm are powers of this field of constants, hence are in some sense minimal extensions.

Even without the notion of prime ideals we can still show interesting relationship between the algebras produced by the algorithm of Theorem 2.8. The plan is to show that any two such algebras \( A \) and \( B \) are essentially isomorphic in the sense that each of them is equal to the power of some common triangular separable algebra \( R \), i.e. \( A \cong R^m \) and \( B \cong R^n \) for some positive integers \( m, n \). To show that \( A \cong R^m \) we have to be able to decompose \( A \). To do this we need to constructively obtain a system of orthogonal
nontrivial (unless \( A \cong R \) already) idempotents \( e_1, ..., e_m \). Since \( A \) and \( B \) split each other, the composition of these maps gives a homomorphism from \( A \) to itself. We know that a homomorphism between a field and itself is an automorphism thus as we would expect if there is a homomorphism from a triangular separable algebra \( A \) to itself that is not an automorphism we can decompose this algebra non trivially. We use the composition of the split maps from \( A \) to \( B \) and vice versa as our homomorphism this will enable us to repeat the process after the initial decomposition, that is if \( A/e_1, B/e_2 \) are algebras in the decompositions of \( A \) and \( B \), respectively, we know that they split each other. This process of decomposition stops once we reach the common algebra \( R \).

**Lemma 3.13** Let \( A \) be a triangular separable algebra over a field \( K \) and let \( \pi : A \to A \) be \( K \)-homomorphism. Then \( \pi \) is either an automorphism of \( A \) or we can find a non-trivial decomposition \( A \cong A_1 \times \ldots \times A_l \).

**Proof** Let \( A = K[a_1, ..., a_l], p_1, ..., p_l \) with \( \deg(p_i) = n_i, 0 < i \leq l \). Let \( \pi \) map \( a_i \) to \( \bar{a}_i \), for \( 0 < i \leq l \). Then \( \bar{a}_1 \) is a root of \( p_1(X), \bar{a}_2 \) is a root of \( \pi(p_2) = \bar{p}_2 = p_2(\bar{a}_1, X) \) etc.

In general \( \bar{a}_i \) is a root of \( \pi(p_i) = \bar{p}_i = p_i(\bar{a}_1, ..., \bar{a}_{i-1}, X) \). The set of vectors \( S = \{ \bar{a}_1^{i_1} \bar{a}_2^{i_2} | 0 \leq i_j < n_j, 0 < j \leq l \} \) is a basis for the vector space \( A \) over \( K \). If the image \( \pi(S) = \bar{S} = \{ \bar{a}_1^{i_1} \bar{a}_2^{i_2} | 0 \leq i_j < n_j, 0 < j \leq l \} \) is a basis for \( A \), i.e. the vectors in \( \bar{S} \) are linearly independent then \( \pi \) is surjective and thus an automorphism.

Assuming \( \pi \) is not an automorphism, we must have a linear dependence relation of the vectors in \( \bar{S} \). We can test if the vectors \( 1, \bar{a}_1, ..., \bar{a}_1^{n_1-1} \) are linearly dependent, and then test if the vectors \( \{ \bar{a}_1^{i_1} \bar{a}_2^{i_2} | 0 \leq i_1 < i_2, 0 \leq i_2 < n_2 \} \) are linearly dependent etc.

In general for some \( s < l \) let the set \( V_s = \{ \bar{a}_1^{i_1} \bar{a}_s^{i_s} | 0 \leq i_j < n_j, 0 < j \leq s \} \) be a set of linearly independent vectors i.e. \( A_s = K[a_1, ..., a_s] \cong K[\bar{a}_1, ..., \bar{a}_s] \) and the set \( \{ \bar{a}_1^{i_1} \bar{a}_s^{i_s} | 0 \leq i_j < n_j, 0 < j \leq s+1 \} \) be a set of linearly dependent vectors. Then we have a linear dependence relation \( q(\bar{a}_1, ..., \bar{a}_{s+1}) = 0 \) such that the coefficient of \( \bar{a}_s^{\ell} \) for some \( \ell > 0 \) is non zero. Let \( q = q(a_1, ..., a_s, X) \) since \( A_s \cong K[\bar{a}_1, ..., \bar{a}_s], \) the coefficient of \( X^{\ell} \) in \( q \) is non-zero, hence \( q \) is a non-constant polynomial in \( A_s[X] \). We compute the gcd of \( p_{s+1} \) and \( q \) to get \( r, s, q_1, t, g \in A_s[X] \) such that \( p_{s+1} = tg, q = q_1g \) and \( rt + sq_1 = 1 \). We can assume w.l.o.g. that \( g, t \) are both monic since if the leading coefficient of either \( g \) or \( t \) is a non-unit we have a non-trivial decomposition of \( A \). Let \( \bar{g} = \pi(g), \bar{t} = \pi(t), \bar{s} = \pi(s), \bar{q}_1 = \pi(q_1) \) and \( \bar{r} = \pi(r) \). Then \( \pi(p_{s+1}) = \bar{p}_{s+1} = \bar{t}\bar{g}, \bar{q} = \bar{q}_1\bar{g} \) and \( \bar{r} + \bar{s}\bar{q}_1 = 1 \) Since \( \bar{a}_{s+1} \) is a root of both \( \bar{p}_{s+1} \) and \( \bar{q} \) then \( \bar{g}(\bar{a}_{s+1}) = 0 \) and \( \bar{g} \), hence \( g \), is a non-constant polynomial. Since \( \deg(q) < \deg(p_{s+1}) \) then \( \deg(g) < \deg(p_{s+1}) \). Thus we can decompose \( A \) as \( A \cong A/(t) \times A/(g) \) where both \( A/(t) \) and \( A/(g) \) are non-trivial. \( \square \)
Theorem 3.14  Let $A, B$ be triangular separable algebras over a field $K$ such that $A$ splits $B$ and $B$ splits $A$. Then there exist a triangular separable algebra $R$ over $K$ and two positive integers $m, n$ such that $A \cong R^m$ and $B \cong R^n$.

Proof  First we note that by Corollary 3.9 if $A$ splits $B$ then $A$ splits any refinement of $B$. Trivially if $A$ splits $B$ then any refinement of $A$ splits $B$. Since $A$ and $B$ split each other then there is $K$–homomorphisms $\vartheta : B \to A$ and $\varphi : A \to B$. The maps $\pi = \vartheta \circ \varphi$ and $\varepsilon = \varphi \circ \vartheta$ are $K$–homomorphisms from $A$ to $A$ and $B$ to $B$ respectively. If both $\pi$ and $\varepsilon$ are automorphisms then we are done. Otherwise, by Lemma 3.13 we can find a decomposition of either $A$ or $B$. By induction on $\dim(A) + \dim(B)$ the statement follows. 

Theorems 3.14 and 3.11 show that the algebras obtained by the algorithm of Theorem 2.8 are equal to the power of some common algebra. This common triangular separable algebra is an approximation, for lack of irreducibility test for polynomials, of the normal field extension of $K$ generated by the coefficients of the Puiseux expansions $\eta_i \in \tilde{K}[[X^{1/m}]]$ of $F$, where $\tilde{K}$ is the algebraic closure of $K$.

The following are examples from a Haskell implementation of the algorithm. We truncate the different factors unevenly for readability.

Example 3.1  Applying the algorithm to $F(X, Y) = Y^4 - 3Y^2 + XY + X^2 \in Q[X][Y]$ we get.

- $Q[a, b, c], a = 0, b^2 - 13/36 = 0, c^2 - 3 = 0$
  $F(X, Y) =$
  $Y + (-b - 1/6)X + (-31b/351 - 7/162)X^3 + (-415b/41067 - 29/1458)X^5 + ...$ 
  $Y + (b - 1/6)X + (31b/351 - 7/162)X^3 + (1415b/41067 - 29/1458)X^5 + ...$ 
  $Y - c + X/6 + 5cX^2/72 + 7X^3/162 + 185cX^4/10368 + 29X^5/1458 + ...$ 
  $Y + c + X/6 - 5cX^2/72 + 7X^3/162 - 185cX^4/10368 + 29X^5/1458 + ...$

- $Q[a, b, c], a^2 - 3 = 0, b - a/3 = 0, c^2 - 13/36 = 0$
  $F(X, Y) =$
  $Y - a + X/6 + 5aX^2/72 + 7X^3/162 + 185aX^4/10368 + 29X^5/1458 + ...$ 
  $Y + (-c - 1/6)X + (-31c/351 - 7/162)X^3 + (-415c/41067 - 29/1458)X^5 + ...$ 
  $Y + (c - 1/6)X + (31c/351 - 7/162)X^3 + (1415c/41067 - 29/1458)X^5 + ...$ 
  $Y + a + X/6 - 5aX^2/72 + 7X^3/162 - 185aX^4/10368 + 29X^5/1458 + ...$
• $Q[a, b, c], a^2 - 3 = 0, b + 2a/3 = 0, c^2 - 13/36 = 0$

$F(X, Y) =$

$(Y - a + X/6 + 5aX^2/72 + 7X^3/162 + 185aX^4/10368 + 29X^5/1458 + ...)$

$(Y + a + X/6 - 5aX^2/72 + 7X^3/162 - 185aX^4/10368 + 29X^5/1458 + ...)$

$(Y + (-c - 1/6)X + (-31c/351 - 7/162)X^3 + (-415c/41067 - 29/1458)X^5 + ...)$

$(Y + (c - 1/6)X + (31c/351 - 7/162)X^3 + (1415c/41067 - 29/1458)X^5 + ...)$

The algebras in the above example can be readily seen to be isomorphic. However, as we will show later, this is not always the case.

**Example 3.2** Applying the algorithm to $F(X, Y) = Y^5 - 7Y^4 + 13Y^3 + 5Y^2 - 30Y + 18 + X Y Q[X][Y]$ we get.

• $Q[a, b, c, d], a - 8/5 = 0, b^2 + 3/14 = 0, c^3 - 7c/3 + 34/27 = 0,$
  $d^2 + 3c^2/4 - 7/3 = 0$

$F(X, Y) = (Y - 3 - bX^{1/2} - 43X/392 + 7621bX^{3/2}/65856 + 4427X^3/134456 + ...)$

$(Y - 3 + bX^{1/2} - 43X/392 - 7621bX^{3/2}/65856 + 4427X^3/134456 + ...)$

$(Y - c - 1/3 + (129c^2/196 + 30c/49 - 559/588)X + ...)$

$(Y - d + c/2 - 1/3 +$  
  $(-129cd/196 + 30d/49 - 129c^2/392 - 15c/49 + 86/147)X + ...)$

$(Y + d + c/2 - 1/3 +$  
  $(129cd/196 - 30d/49 - 129c^2/392 - 15c/49 + 86/147)X + ...)$

• $Q[a, b, c, d], a^3 + 16a^2/5 + 27a/25 - 2/125 = 0, b - a/4 - 8/5 = 0,$
  $c^2 + 3/14 = 0, d^2 + 3a^2/4 + 8a/5 - 37/25 = 0$

$F(X, Y) = (Y - a - 7/5 + (129a^2/196 + 49a/245 + 2211/4900)X + ...)$

$(Y - 3 - cX^{1/2} - 43X/392 + 7621cX^{3/2}/65856 + 4427X^3/134456 + ...)$

$(Y - 3 + cX^{1/2} - 43X/392 - 7621cX^{3/2}/65856 + 4427X^3/134456 + ...)$

$(Y - d + a/2 + 1/5 +$  
  $(-129ad/196 - 22d/245 - 129a^2/392 - 247a/245 - 142/1225)X + ...)$

$(Y + d + a/2 + 1/5 +$  
  $(129ad/196 + 22d/245 - 129a^2/392 - 247a/245 - 142/1225)X + ...)$
The following are two of the several triangular separable algebras obtained by our Example 3.3 algorithm along with their respective factorization of

\[ F_{18} \]

\[ F \cdot (X \cdot (X \cdot (X - Y) + Y) - Y) = 3 + dX^{1/2} - 43X/392 - 7621dX^{3/2}/65856 + 4427X^2/134456 + ... \]

\[ F(X, Y) = (Y - a - 7/5 + (129a^2/196 + 494a/245 + 2211/4900)X + ...) \]

\[ (Y + b + a/4 - 7/5+) \]

\[ (-129ab/196 - 22b/245 - 387a^2/784 - 1021a/490 - 318/1225)X + ...) \]

\[ (Y - 3 - dX^{1/2} - 43X/392 + 7621dX^{3/2}/65856 + 4427X^2/134456 + ...) \]

\[ (Y + b + 3a/4 + 9/5+) \]

\[ (129ab/196 + 22b/245 - 129a^2/784 + 33a/490 + 34/1225)X + ...) \]

\[ Q[a, b, c, d], a^3 + 16a^2/5 + 27a/25 - 2/125 = 0, \]

\[ b^2 + ab/2 + 16b/5 + 13a^2/16 + 12a/5 + 27/25 = 0, \]

\[ c - b/3 - a/4 - 8/5 = 0, d^2 + 3/14 = 0 \]

\[ F(X, Y) = (Y - a - 7/5 + (129a^2/196 + 494a/245 + 2211/4900)X + ...) \]

\[ (Y + b + a/4 - 7/5+) \]

\[ (-129ab/196 - 22b/245 - 387a^2/784 - 1021a/490 - 318/1225)X + ...) \]

\[ (Y + b + 3a/4 + 9/5+) \]

\[ (129ab/196 + 22b/245 - 129a^2/784 + 33a/490 + 34/1225)X + ...) \]

\[ (Y - 3 - dX^{1/2} - 43X/392 + 7621dX^{3/2}/65856 + 4427X^2/134456 + ...) \]

\[ (Y - 3 - dX^{1/2} - 43X/392 - 7621dX^{3/2}/65856 + 4427X^2/134456 + ...) \]

Example 3.3  To illustrate Theorem 3.14 we show how it works in the context of an example computation. The polynomial is \( F(X, Y) = Y^6 + X^6 + 3X^2Y^4 + 3X^4Y^2 - 4X^2Y^2 \). The following are two of the several triangular separable algebras obtained by our algorithm along with their respective factorization of \( F(X, Y) \).
We now show that the two algebras indeed split each other. Over $B$ the polynomial $p_1$ factors as $p_1 = (Y - r)(Y + r)(Y - w)(Y + w)$. Each of these factors partly specify a homomorphism taking $a$ to a zero of $p_1$ in $B$. For each we get a factorization of $p_4$ over $B$.

- $a \mapsto r$
  
  $p_4 = (Y + 2r/3)(Y - w - r/3)(Y + w - r/3)$

- $a \mapsto -r$
  
  $p_4 = (Y - 2r/3)(Y - w + r/3)(Y + w + r/3)$

- $a \mapsto w$
  
  $p_4 = (Y - r - w/3)(Y + r - w/3)(Y + 2w/3)$

- $a \mapsto -w$
  
  $p_4 = (Y - r + w/3)(Y + r + w/3)(Y - 2w/3)$
For each of the 4 mappings of \( a \) we get 3 mappings of \( d \). Now we see we have 12 different mappings arising from the different mappings of \( a \) and \( d \). Each of these 12 mappings will give rise to 2 different mappings of \( e \) (factorization of \( p_5 \))...etc. Thus we have a number of homomorphisms equal to the dimension of the algebra, that is 48 homomorphisms. We avoid listing all these homomorphisms here. In conclusion, we see that \( B \) splits \( A \). Similarly, we have that \( A \) splits \( B \). We show only one of the 16 homomorphisms below. The polynomial \( q_1 \) factors linearly over \( A \) as \( q_1 = (Y - a)(Y - d + a/3)(Y - e + d/2 + a/3)(Y + e + d/2 + a/3) \). Under the map \( r \leftrightarrow a \) we get a factorization of \( q_5 \) over \( A \) as

\[
q_5 = Y^2 + a^2 = (Y - a^2 d^2 e/8 + a^3 d e/12 - 5e/9 - a^3 d^2 /8 - 2d/3 - 2a/9) \\
(Y + a^2 d^2 e/8 - a^3 d e/12 + 5e/9 + a^3 d^2 /8 + 2d/3 + 2a/9)
\]

Now to the application of Theorem 3.14. Under the map above we have an endomorphism \( a \mapsto r \mapsto a \) and \( d \mapsto -2r/3 \mapsto -2a/3 \). Thus in the kernel we have the nonzero element \( d + 2a/3 \) and as expected \( Y + 2a/3 \) divides \( p_4 \). Using this we obtain a decomposition of \( A \cong A_1 \times A_2 \). We have \( A_1 = Q[a, b, c, d, e], p_1, p_2, p_3, g_4, p_5 \) with \( g_4 = Y + 2a/3 \) and \( A_2 = Q[a, b, c, d, e], p_1, p_2, p_3, h_4, p_5 \) with \( h_4 = Y^2 - 2aY/3 + 10a^2/9 \).

With \( d + 2a/3 = 0 \) in \( A_1 \), \( p_5 = Y^2 + 3d^2/4 + 2a^2/3 = Y^2 + a^2 \) and we can see immediately that \( A_1 \cong B \). Similarly, we can decompose the algebra \( A_2 \cong C_1 \times C_2 \), where \( C_1 = Q[a, b, c, d, e], p_1, p_2, p_3, h_4, g_5 \) with \( g_5 = Y - d/2 + 2a/3 \) and \( C_2 = Q[a, b, c, d, e], p_1, p_2, p_3, h_5, h_5 \) with \( h_5 = Y + d/2 - 2a/3 \). The polynomial \( q_5 \) factors linearly over both \( C_1 \) and \( C_2 \) as \( q_5 = (Y - d + a/3)(Y + d - a/3) \). We can readily see that both \( C_1 \) and \( C_2 \) are isomorphic to \( B \), through the \( C_1 \) automorphism \( a \mapsto r \mapsto a, d \mapsto w + r/3 \mapsto d \). Thus proving \( A \cong B^3 \).

4 Acknowledgments

We thank the referees for comments and suggestions that helped to improve the article.

The research leading to the results presented here has been supported by ERC Advanced grant project 247219.

References


[8] S I Newton. The method of fluxions and infinite series: with its application to the geometry of curve-lines, printed by Henry Woodfall; and sold by John Nourse (1736)


Department of Computer Science and Engineering, University of Gothenburg
SE-412 96, Gothenburg, Sweden

Department of Computer Science and Engineering, University of Gothenburg
SE-412 96, Gothenburg, Sweden

bassel.manna@cse.gu.se, thierry.coquand@cse.gu.se


Received: aa bb 20YY Revised: cc dd 20ZZ